

441 G St. N.W.
Washington, DC 20548

Accessible Version

May 4, 2021

The Honorable Charles P. Rettig
Commissioner of the Internal Revenue Service

Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls

Dear Mr. Rettig:

On November 10, 2020, we issued our audit report on Internal Revenue Service's (IRS) fiscal years 2020 and 2019 financial statements, which included our opinion that although controls could be improved, IRS maintained, in all material respects, effective internal control over financial reporting as of September 30, 2020.¹ In that report, we identified two continuing significant deficiencies² in internal control over financial reporting related to unpaid assessments³ and financial reporting systems.

This report presents new control deficiencies we identified during our fiscal year 2020 testing of IRS's controls and one recommendation that is not sensitive in nature. This report also presents the results, as of September 30, 2020, of our follow-up on the status of the agency's corrective actions to address our recommendations detailed in our previous management reports that remained open as of September 30, 2019.⁴ This report is intended for IRS management's use.

This report is a public version of a LIMITED OFFICIAL USE ONLY report that we issued concurrently.⁵ IRS deemed much of the information in the LIMITED OFFICIAL USE ONLY report to be sensitive information, which must be protected from public disclosure. Therefore, this report omits sensitive information about the deficiencies. Although the information provided in this report is

¹GAO, *Financial Audit: IRS's FY 2020 and FY 2019 Financial Statements*, [GAO-21-162](#) (Washington, D.C.: Nov. 10, 2020).

²A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

³An unpaid assessment is a legally enforceable claim against a taxpayer and consists of taxes, penalties, and interest that have not been collected or abated (i.e., IRS has reduced the assessment). See, for example, implementing guidance in the *Internal Revenue Manual* § 1.34.4.1.6(1.p), Terms/Definitions (Aug. 25, 2015).

⁴GAO, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Internal Control over Financial Reporting*, [GAO-20-480R](#) (Washington, D.C.: May 1, 2020). GAO, *Management Report: Improvements Are Needed to Enhance the Internal Revenue Service's Information System Security Controls*, [GAO-20-410RSU](#) (Washington, D.C.: May 13, 2020).

⁵GAO, *Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls*, [GAO-21-400RSU](#) (Washington, D.C.: May 4, 2021).

more limited, the report addresses the same objectives as the LIMITED OFFICIAL USE ONLY report and uses the same methodology.

Results in Brief

During our fiscal year 2020 audit, we identified new information system control deficiencies related to access controls and security management that contributed to IRS's continuing significant deficiency in its internal control over financial reporting systems. These new deficiencies, along with unresolved information system control deficiencies from our prior audits, increase the risk of unauthorized access to, modification of, or disclosure of financial reporting and taxpayer data and disruption of critical operations. We also identified a new control deficiency related to tax credits that although not considered a material weakness or significant deficiency, nonetheless warrants IRS management's attention in order to help reduce the risk of erroneous and fraudulent refund disbursements.

We are making one recommendation in this report to address the control deficiency in security management. Enclosure I provides the detailed control deficiency and associated recommendation. In the LIMITED OFFICIAL USE ONLY report, we are making five recommendations: four recommendations to address control deficiencies in access controls and one recommendation to address the control deficiency in tax credits.

In addition, we determined that IRS had completed corrective actions to close 48 of 162 recommendations from our prior audits related to control deficiencies that remained open as of September 30, 2019. Specifically, IRS's actions addressed

- four of 13 transaction cycle recommendations,⁶
- 41 of 132 information system recommendations, and
- three of 17 safeguarding recommendations.⁷

Therefore, including prior and new recommendations, the agency currently has the following outstanding recommendations to address:

- 10 transaction cycle recommendations, which consist of nine prior recommendations and one new recommendation related to tax credits that we are making in the LIMITED OFFICIAL USE ONLY report;
- 96 information system recommendations, which consists of 91 prior recommendations, one new recommendation related to security management that we are making in this report, and four new recommendations related to access controls that we are making in the LIMITED OFFICIAL USE ONLY report; and
- 14 safeguarding recommendations.

Enclosure II provides the 41 open recommendations that are not sensitive in nature from our prior audits and their status as of September 30, 2020. The LIMITED OFFICIAL USE ONLY

⁶A transaction cycle is a set of business transactions that process control activities to provide reasonable assurance that relevant financial statement assertions are met.

⁷Safeguarding is the processes and controls involved in protecting custodial and noncustodial assets, which includes the prevention of loss, theft, and inappropriate disclosure or misuse by employees and other individuals. Custodial and noncustodial assets consist of (1) electronic and hard-copy taxpayer receipts, (2) taxpayer information, (3) facilities (e.g., campuses, lockbox banks, computing centers, field offices, etc.), (4) general property and equipment, and (5) other nontax collections and receipts.

report contains the open recommendations that are sensitive and not sensitive in nature from our prior audits and their status as of September 30, 2020.

In commenting on a draft of this report, IRS agreed with our recommendation and stated that it is committed to implementing improvements dedicated to promoting the highest standard of financial management, internal controls, and information technology security. IRS's comments are reproduced in enclosure III.

Objectives, Scope, and Methodology

Our objectives were to

- evaluate IRS's internal control over financial reporting⁸ and
- determine the status of the agency's corrective actions as of September 30, 2020, to address recommendations in our prior years' reports for which actions were not complete as of September 30, 2019.

We performed this work in connection with our audit of IRS's financial statements for the fiscal years ended September 30, 2020, and 2019, to support our opinion on whether the agency maintained, in all material respects, effective internal control over financial reporting.

To accomplish these objectives, we tested relevant controls for proper authorizing, executing, accounting, and reporting of transactions and for safeguarding assets and taxpayer information. We also reviewed applicable agency policies and procedures, observed operations, tested generalizable and nongeneralizable samples of transactions, examined relevant documents and records, and interviewed IRS management and staff. For our evaluation of IRS's internal control over financial reporting related to information systems, we focused on relevant financial and tax processing systems that support the processing, storage, and transmission of financial and sensitive taxpayer information.

We based our evaluation on the *Financial Audit Manual*⁹ and *Federal Information System Controls Audit Manual*.¹⁰

During the course of our work, we communicated our findings to IRS management (see enc. I). We will follow up with the agency to determine the status of corrective actions taken on the remaining recommendations reported as open in this report (see enc. II) during our fiscal year 2021 audit of IRS's financial statements.

⁸An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, the objectives of which are to provide reasonable assurance that (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with U.S. generally accepted accounting principles, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition, and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the financial statements.

⁹GAO, *Financial Audit Manual Volume 1*, [GAO-18-601G](#) (June 2018, updated April 2020), contains the methodology for performing financial statement audits of federal entities in accordance with professional auditing and attestation standards and Office of Management and Budget guidance.

¹⁰GAO, *Federal Information System Controls Audit Manual (FISCAM)*, [GAO-09-232G](#) (Washington, D.C.: February 2009), contains the guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of information and information systems.

We performed our audit in accordance with U.S. generally accepted government auditing standards. We believe that our audit provides a reasonable basis for our finding and recommendation in this report and our findings and recommendations in our separately issued LIMITED OFFICIAL USE ONLY report.

New Deficiencies Identified in IRS’s Internal Control over Financial Reporting

During our IRS fiscal year 2020 audit, we identified new control deficiencies in internal control over financial reporting in information systems related to access controls and security management that contributed to our reported continuing significant deficiency in IRS’s internal control over financial reporting systems. Additionally, we identified a new control deficiency in internal control over financial reporting related to tax credits that although not considered a material weakness or significant deficiency, warrants management’s attention.

We are making one recommendation in this report to address a deficiency in security management. Because of the sensitive nature involved with the deficiencies surrounding access controls and tax credit controls, we summarize these deficiencies in this report, while our LIMITED OFFICIAL USE ONLY report provides a more detailed discussion of these deficiencies along with five recommendations: four related to access controls and one related to tax credits.

Access Controls

A basic management objective for any agency is to protect the resources that support its critical operations from unauthorized access. An agency accomplishes this by designing and implementing controls to prevent, limit, and detect unauthorized access to programs, data, facilities, and other computing resources. Access controls include both logical and physical controls related to (1) protection of system boundaries, (2) identification and authentication, (3) authorization of access permissions, (4) cryptography, (5) audit and monitoring of system activity, and (6) physical security of facilities and computing resources.¹¹ Appropriately designed and implemented access controls reduce the risk of unauthorized access to, modification of, or disclosure of financial reporting and taxpayer data and disruption of critical operations.

The three deficiencies in access controls we identified during our fiscal year 2020 audit related to (1) identification and authentication and (2) cryptography.

Identification and Authentication

Identification is the process of distinguishing one user from others as a prerequisite for granting access to resources in an information system. User identification (ID) is important because a system uses it to assign and recognize specific access privileges. However, the confidentiality of a user ID is typically not protected. For this reason, agencies may use other means of authenticating users—that is, determining whether individuals are who they claim to be—such as with the use of tokens or biometrics. Appropriately designed and implemented identification and authentication controls require users to authenticate themselves using personal identity verification (PIV) card credentials and other identifiers, such as passwords.¹²

¹¹Cryptography involves the encryption of information.

¹²A PIV card is a physical identity card, such as a “smart” card, issued to an individual. It contains stored identity credentials, such as a photograph, cryptographic keys, or digitized fingerprint used to verify the identity of the cardholder against the stored credentials by another person or an automated process. A PIV certificate can be used for authentication to verify that PIV credentials were issued by an authorized entity, were not expired, and were not revoked and that the holder of the credentials was the same individual to whom the PIV card was issued.

We identified two deficiencies in access controls related to identification and authentication. IRS did not

- remove certain accounts in accordance with agency policy and
- consistently record the correct access revoke date for certain users to a system environment that processes taxpayer data.

Cryptography

Cryptography controls can be used in identification and authorization to protect the integrity and confidentiality of computer programs and data in transmission or storage. Using algorithms (mathematical functions) and keys (strings of seemingly random bits), cryptographic modules¹³ (1) encrypt a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential; (2) provide an electronic signature that can be used in a file to determine whether any changes have been made, thus providing reasonable assurance of the file's integrity; or (3) link a message or document to a specific individual's or group's key, thus ensuring that the "signer" of the file can be identified. Appropriately designed and implemented encryption controls can help prevent unauthorized access and disclosure of information (confidentiality) and detect changes to information (integrity).

We identified one deficiency in access controls related to cryptography (i.e., encryption). IRS did not enforce cryptographic protocols used for authentication and data integrity in a system environment that processes taxpayer data in accordance with agency policy and National Institute of Standards and Technology guidance.

Security Management

Security management is the foundation of a security control structure and reflects senior management's commitment to addressing security risks. An effective security management program provides a framework and continuous cycle of activity for assessing risk, developing and implementing security procedures, and monitoring the effectiveness of these procedures. Without a well-designed security management program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

We identified one deficiency in security management related to external system risk assessments. IRS did not conduct an adequate assessment of risks and controls of an external system (see enc. I).

Tax Credits

Congress provides tax credits and other outlays as assistance to targeted individuals and businesses. Any individual or business that meets certain requirements becomes eligible for a tax credit and can claim it when filing a federal tax return. There are two types of tax credits: nonrefundable and refundable. A nonrefundable tax credit is limited to the taxpayer's tax liability, while a refundable tax credit is fully payable to the taxpayer, even if the tax credit exceeds the taxpayer's tax liability. Appropriately designed and implemented controls over tax credits can help reduce the risk of erroneous and fraudulent refund disbursements related to tax credits.

¹³A cryptographic module is the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including algorithms, and is contained within the encrypted boundary of the module.

During fiscal year 2020, the CARES Act was enacted; it contained a number of provisions to help stimulate the economy, including a one-time payment (Economic Impact Payment (EIP)) of up to \$500 per child for taxpayers who are eligible for the Child Tax Credit (CTC).¹⁴ To calculate the EIP for qualifying children, IRS relied on the total number of CTC-qualifying children claimed on a tax return. We tested IRS's controls over the processing of EIPs to determine whether the agency complied with the EIP provisions of the CARES Act.¹⁵

We identified one deficiency in processing tax credits. IRS did not consistently validate certain information on the CTC claims that taxpayers submitted.

Status of Prior Audit Recommendations

IRS has continued to address many of the control deficiencies related to open recommendations from our prior audits. As of September 30, 2019, there were 13 transaction cycle recommendations, 132 information system recommendations, and 17 safeguarding recommendations from prior year audits that we reported as open in our status of recommendations in the management reports issued in May 2020.¹⁶ During our fiscal year 2020 audit, we determined the following:

- IRS completed corrective actions to address four of the 13 transaction cycle recommendations from our prior audits. As a result, the agency needs to address 10 transaction cycle recommendations—nine from our prior audits and one new recommendation related to tax credits that we are making in the LIMITED OFFICIAL USE ONLY report.
- IRS completed corrective actions to address 41 of the 132 information system recommendations from our prior audits. As a result, the agency needs to address 96 information system recommendations—91 from our prior audits, one new recommendation related to security management that we are making in this report, and four new recommendations related to access controls that we are making in the LIMITED OFFICIAL USE ONLY report.
- IRS completed corrective actions to address three of the 17 safeguarding recommendations from our prior audits. As a result, the agency needs to address 14 safeguarding recommendations.

See table 1 for a summary of the status of our prior recommendations and enclosure II for the status of each of our prior recommendations.

¹⁴Pub. L. No. 116-136, div. A, § 2201, 134 Stat. 281, 335–340 (Mar. 27, 2020), *codified at* 26 U.S.C. § 6428(a).

¹⁵We tested 289 EIP transactions that IRS processed from April 10 through May 29, 2020. These transactions consisted of a monetary unit sample of 112 EIPs, totaling \$230,264, as well as 177 EIPs that were greater than or equal to \$8,000, totaling approximately \$1.6 million.

¹⁶[GAO-20-480R](#) and [GAO-20-410RSU](#).

Table 1: Status of GAO Recommendations to IRS Related to Internal Control over Financial Reporting

Transaction cycles

Audit area	Open recommendations from prior audits as of September 30, 2019	Prior recommendations closed as of September 30, 2020	New recommendations resulting from FY 2020 audit	Total remaining open recommendations
Unpaid assessments	2	1	—	1
Tax outlays Refunds	7	2	—	5
Tax outlays Tax credits	1	—	1	2
Total (tax outlays)	8	2	1	7
Property and equipment	1	—	—	1
Nonpayroll	2	1	—	1
Total (transaction cycles)	13	4	1	10

Nontransaction cycles

Audit area		Open recommendations from prior audits as of September 30, 2019	Prior recommendations closed as of September 30, 2020	New recommendations resulting from FY 2020 audit	Total remaining open recommendations
Information systems	Access control Boundary protection	8	3	—	5
	Access control Identification and authentication	37	18	2	21
	Access control	13	7	—	6
	Access control	24	2	2	24
	Access control	10	3	—	7
	Total (access controls)	92	33	4	63
	Configuration management	30	4	—	26
	Segregation of duties	2	1	—	1
Security management	8	3	1	6	
Total (information systems)	132	41	5	96	
Safeguarding	Safeguarding	17	3	—	14
Total	Total (nontransaction cycles)	149	44	5	110
Total Transaction and Non-transaction	Total	162	48	6	120

Legend: FY = fiscal year; — = no recommendations made.

Source: GAO analysis of Internal Revenue Service (IRS) data. | GAO-21-401R

Recommendations for Executive Action

To help strengthen internal control over financial reporting, we are making one recommendation to address a new deficiency related to security management that we discuss in this report (see enc. I) and five recommendations to address new deficiencies in access controls and tax credits that we discuss in our separately issued LIMITED OFFICIAL USE ONLY report.

Agency Comments

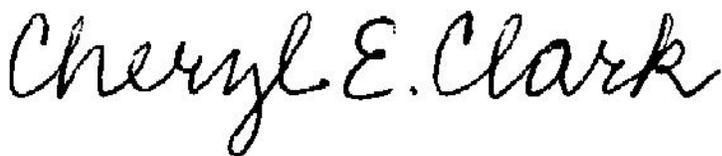
We provided a draft of this report to IRS for comment. In its comments, reproduced in enclosure III, IRS agreed with our recommendation and provided planned actions to address our finding. IRS also stated that it is committed to implementing improvements dedicated to promoting the highest standard of financial management, internal controls, and information technology security. We will evaluate the effectiveness of IRS's efforts during our audit of its fiscal year 2021 financial statements.

This report contains a recommendation to the Commissioner of the Internal Revenue Service. The head of a federal agency is required by 31 U.S.C. § 720 to submit a written statement on actions taken or planned on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Oversight and Reform, the congressional committees with jurisdiction over the agency programs and activities that are the subject of our recommendations, and GAO not later than 180 days after the date of this report. A written statement must also be sent to the Senate and House Committees on Appropriations with the agency's first request for appropriations made more than 180 days after the date of this report.

We are sending copies of this report to Department of the Treasury officials in the Office of the Secretary, the Treasury Inspector General for Tax Administration, and appropriate congressional committees. In addition, this report is available at no charge on the GAO website at <https://www.gao.gov>.

We acknowledge and appreciate the cooperation and assistance from IRS officials and staff during our audit of IRS's fiscal years 2020 and 2019 financial statements. If you or your staff have any questions about this report, please contact Cheryl E. Clark at (202) 512-9377 or clarkce@gao.gov or Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report include Mark Canter (Assistant Director), Sher'rie Bacon, Kisa Bushyeager, Liliam Coronado, Joseph Crays, Nina Crocker, Larry Crosland, Kristi Dorsey, Nancy Glover, Tyrone Hutchins, J. Andrew Long, Vernetta Marquis, Kevin Metcalfe, Koushik Nalluru, and Eugene Stevens.

Sincerely yours,



Cheryl E. Clark
Director, Financial Management and Assurance



Vijay A. D'Souza
Director, Information Technology and Cybersecurity

Enclosures - 3

Enclosure I

New Deficiencies in IRS's Internal Control over Financial Reporting

This enclosure presents detailed information on the new deficiency in internal control over financial reporting in information systems related to security management identified during our audit of the Internal Revenue Service's (IRS) fiscal years 2020 and 2019 financial statements.¹ This enclosure also includes our recommendation that if effectively implemented should mitigate or correct the deficiency.

Security Management

Risk Assessments

External System Controls and Risk Were Not Adequately Assessed

Condition. IRS did not conduct an adequate assessment of risks and controls of an external system. The agency stated that it had reviewed the current service organization controls report on an external system. However, we found that the agency based part of its initial assessment of the external system's control environment, including control deficiencies and risks, on a prior service organization controls report review before the issuance of the current year's service organization controls report.

Criteria. IRS External Systems Review Procedures direct IRS to assess external systems annually and, when available, review those systems' System and Organization Controls report.

National Institute of Standards and Technology Special Publication 800-53, revision 4, requires that an organization accepts the results of an assessment of an information system that an external organization performed when the assessment meets the organization's requirements.²

¹An entity's internal control over financial reporting is a process effected by those charged with governance, management, and other personnel, the objectives of which are to provide reasonable assurance that (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with U.S. generally accepted accounting principles and that assets are safeguarded against loss from unauthorized acquisition, use, or disposition, and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the financial statements.

²National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 4 (Gaithersburg, Md.: April 2013).

Enclosure I

Cause. The IRS official performing the review incorrectly referenced the wrong version of the service organization controls report in the review form. Furthermore, IRS management approved the evaluation without making sure that the service organization controls report had a second review.

Effect. As a result, IRS increases its risk of not adequately assessing risks and control deficiencies that affect its control environment for fiscal year 2020.

Recommendation for Executive Action. The Commissioner of the Internal Revenue Service should reasonably assure that reviews of external third parties' systems reference current documentation that supports IRS assessments of risk. (Recommendation 1)

Enclosure II

Enclosure II

Status of Previously Reported Recommendations

Our fiscal year 2020 audit included following up on the status of the Internal Revenue Service's (IRS) corrective actions to address recommendations from our prior audits that remained open at the beginning of our fiscal year 2020 audit. Table 2 shows the status of these 41 previously reported recommendations that are not sensitive in nature as of September 30, 2020. The LIMITED OFFICIAL USE ONLY report contains recommendations that are sensitive in nature from our prior audits and their status as of September 30, 2020. We will continue to evaluate the agency's actions to address recommendations that remain open during future audits. We define the abbreviations used in the legend at the end of the table.

Table 2: Status of Previously Reported Recommendations as of September 30, 2020

Transaction cycles

	No.	Source report and recommendation number	Recommendation	Recommendation status
Unpaid assessments	1.	GAO-18-393R, #18-02	Based on IRS's research and determination, design and implement the corrective actions necessary to reasonably assure that IRS effectively resolves and records unpostable transactions in a timely manner, including establishing clearly defined time frames in the IRM by which the IRS operating divisions should correct unpostable transactions and appropriate related oversight and review processes.	Closed
	2.	GAO-19-412R, #19-01	Implement the necessary actions to effectively address the two primary causes of the significant deficiency in IRS's internal control over unpaid assessments. These actions should (1) resolve the system limitations affecting the recording and maintenance of reliable and appropriately classified unpaid assessments and related taxpayer data to support timely and informed management decisions, and enable appropriate financial reporting of unpaid assessment balances throughout the year, and (2) identify the control deficiencies that result in significant errors in taxpayer accounts and implement control procedures to routinely and effectively prevent, or detect and correct, such errors.	Open
Refunds	3.	GAO-16-457R, #16-07	Determine the reason(s) why staff did not always comply with IRS's established policies and procedures related to initiating, monitoring, and reviewing the monitoring of manual refunds and, based on this determination, establish a process to better enforce compliance with these requirements.	Open
	4.	GAO-16-457R, #16-10	Identify the cause of and implement a solution for dealing with the periodic backlogs of ICO inventory that is hampering the performance of quality reviews.	Open
	5.	GAO-19-412R, #19-08	Update and implement policies or procedures, or both, to clearly define the roles and responsibilities of second-level managers and IDRS security account administrators for validating the information on USR designation forms, including specifying how the information should be validated.	Open

Enclosure II

	No.	Source report and recommendation number	Recommendation	Recommendation status
	6.	GAO-19-412R, #19-09	Update and implement procedures to clearly specify the tax refund data elements that PVS COs are required to verify before certifying the tax refunds in SPS.	Closed
	7.	GAO-19-412R, #19-10	Establish and implement a review process to provide reasonable assurance that the RSNs that Data Conversion key entry operators enter into the ISRP system and post to the master files are correct.	Closed
	8.	GAO-19-412R, #19-11	Implement a validity check in the ISRP system to confirm that RSNs that Data Conversion key entry operators enter into the system have the required 14 digits.	Open
	9.	GAO-20-480R, #20-02	Establish and implement manual refund procedures to direct (1) initiators to document (e.g., record on the taxpayers' accounts or annotate on the related manual refund forms) the justification for bypassing the IAT tool warning related to potential duplicate tax refunds on taxpayers' accounts and (2) managers to monitor whether such warnings were bypassed and review the justifications for reasonableness prior to approving manual refund forms.	Open
Tax credits	10.	GAO-19-412R, #19-12	Update and implement policies or procedures, or both, to require that reviewers follow up with tax examiners to verify the errors that tax examiners made in working on cases related to suspicious or questionable tax returns are corrected.	Open
Property and equipment	11.	GAO-16-457R, #16-13	Establish and implement monitoring procedures designed to reasonably assure that the key detailed information for tangible capitalized P&E is properly recorded and updated in the KISAM system.	Open
Nonpayroll	12.	GAO-20-480R, #20-03	Establish and implement actions to provide reasonable assurance that business units record the acceptance of goods and services in a timely manner in accordance with IRS policies and procedures.	Open
	13.	GAO-20-480R, #20-04	Establish and implement actions to provide reasonable assurance that the future lease payment amounts for non-cancellable operating leases are calculated correctly.	Closed

Information systems

	No.	Source report and recommendation number	Recommendation	Recommendation status
Authorization	14.	GAO-18-391, #01	Improve the implementation of IRS's information security program by entering correct contractor password expiration dates, per IRS's policy, in the system used for managing user access authorizations.	Closed
	15.	GAO-18-391, #02	Improve the implementation of IRS's information security program by documenting access authorizations for nonunique accounts.	Open
	16.	GAO-18-391, #03	Improve the implementation of IRS's information security program by reviewing nonunique accounts at least annually, per IRS's policy.	Open

Enclosure II

	No.	Source report and recommendation number	Recommendation	Recommendation status
Audit and monitoring	17.	GAO-16-398, #01	Update system and application audit plans based on the current version of referenced policies and guidelines and when significant changes are made to a system or application.	Closed
	18.	GAO-17-395, #01	Implement the audit plans for the 12 systems and applications that we reviewed in the production computing environment.	Open
	19.	GAO-17-395, #02	Ensure that system administrators and security operations analysts are alerted in the event of audit processing failures.	Open
Security management	20.	GAO-15-337, #03	Ensure that control testing methodology and results fully meet the intent of the control objectives being tested.	Closed
	21.	GAO-15-337, #05	Update the remedial action verification process to ensure that actions are fully implemented.	Closed
	22.	GAO-17-395, #07	Regularly update configuration standards and guidelines for network devices to incorporate recommendations from industry leaders, security agencies, and key practices from IRS partners to address known vulnerabilities applicable to IRS's environment.	Open
	23.	GAO-17-395, #08	Implement a compliance verification application or other appropriate process to ensure that configuration policies are comprehensively tested on the mainframe.	Open
	24.	GAO-17-395, #10	Identify and review service organizations' listing of user controls that are deemed relevant and test those controls to appropriately draw conclusions about the operating effectiveness of controls.	Closed

Safeguarding

	No.	Source report and recommendation number	Recommendation	Recommendation status
Safeguarding	25.	GAO-11-494R, #11-24	Revise the post orders for the SCCs and lockbox bank security guards to include specific procedures for timely reporting exterior lighting outages to SCCs or lockbox bank facilities management. These procedures should specify (1) whom to contact to report lighting outages and (2) how to document and track lighting outages until resolved.	Closed
	26.	GAO-13-420R, #13-05	Perform a risk assessment to determine the appropriate level of IDRS access that should be granted to employee groups that handle hard-copy taxpayer receipts and related sensitive taxpayer information as part of their job responsibilities.	Open
	27.	GAO-13-420R, #13-06	Based on the results of the risk assessment, update the IRM accordingly to specify the appropriate level of IDRS access that should be allowed for (1) remittance perfection technicians and (2) all other employee groups with IDRS access that handle hard-copy taxpayer receipts and related sensitive information as part of their job responsibilities.	Open
	28.	GAO-13-420R, #13-07	Establish procedures to implement the updated IRM, including required steps to follow to prevent (1) remittance perfection technicians and (2) all other employee groups that handle hard-copy taxpayer receipts and related sensitive information as part of their job responsibilities from gaining access to command codes not required as part of their designated job duties.	Open

Enclosure II

No.	Source report and recommendation number	Recommendation	Recommendation status
29.	GAO-15-480R, #15-07	Establish procedures to monitor whether non-IRS contractors with unescorted physical access to IRS facilities are receiving unauthorized access awareness training.	Open
30.	GAO-15-480R, #15-08	Determine the reasons why staff did not consistently comply with IRS's existing requirements for the final candling of receipts at SCCs and lockbox banks, including logging remittances found during final candling on the final candling log at the time of discovery, safeguarding the remittances at the time of discovery, transferring the remittances to the deposit unit promptly, and passing one envelope at a time over the light source, and based on this determination, establish a process to better enforce compliance with these requirements.	Open
31.	GAO-17-454R, #17-03	Strengthen the process for reasonably assuring that the IRM is reviewed annually to align with the current control procedures and guidance being implemented by agency personnel. This should include a mechanism for reasonably assuring that program owner directors (1) review their respective program control activities and related guidance annually and timely update the IRM as needed, (2) document their reviews, and (3) utilize interim guidance and supplemental guidance correctly for their intended purposes.	Open
32.	GAO-18-393R, #18-03	Develop and implement policies in the IRM for conducting and monitoring the Submission Processing internal control review. These policies should include or be accompanied by procedures to (1) assess and update the review questions and cited IRM criteria to reasonably assure they align with the controls under review; (2) periodically evaluate and document a review of the error threshold methodology to assess its current validity based on changes to the operating environment; (3) report findings identified in the Findings and Corrective Actions Report; and (4) assess and monitor (a) safeguarding of internal control activities across all work shifts, particularly during peak seasons, (b) safeguarding of internal control activities for the appropriate use and destruction of hard-copy taxpayer information, and (c) the results of relevant functional level reviews.	Open
33.	GAO-18-393R, #18-04	Develop and implement policies in the IRM for conducting and monitoring the AMC review. These policies should include or be accompanied by procedures for IRS management responsible for establishing policies related to safeguarding controls to (1) periodically monitor the results of the review; (2) clarify the minimum requirements for how frequently the review should be completed at its various facilities while considering factors that may affect the most appropriate timing of these reviews, such as changes in personnel, operational processes, or information technology; and (3) reasonably assure that corrective actions for all identified deficiencies are tracked until fully implemented.	Closed
34.	GAO-18-393R, #18-05	Develop and implement policies in the IRM for conducting and monitoring the AEHR review. These policies should include or be accompanied by procedures for IRS management responsible for establishing policies related to safeguarding controls to (1) periodically monitor the results of the review and (2) reasonably assure that corrective actions for all identified deficiencies are tracked until fully implemented.	Open
35.	GAO-19-412R, #19-02	Document and implement a formal comprehensive strategy to provide reasonable assurance concerning its nationwide coordination, consistency, and accountability for internal control over key areas of physical security. This strategy should include nationwide improvements for (1) coordinating among the functional areas involved in physical security; (2) implementing and monitoring the effectiveness of physical security policies, procedures, and internal controls; and (3) ongoing communication in identifying, documenting, and taking corrective action to resolve underlying control issues that affect IRS's facilities.	Open

Enclosure II

No.	Source report and recommendation number	Recommendation	Recommendation status
36.	GAO-19-412R, #19-03	Determine the reasons staff did not consistently comply with IRS's existing requirement for maintaining an emergency contact list at all of its facilities and, based on this determination, establish a process to enforce compliance with the requirement.	Closed
37.	GAO-19-412R, #19-04	Establish and implement policies and procedures requiring that corrective actions be documented in the Alarm Maintenance and Testing Certification Report for malfunctioning alarms identified in the annual alarm tests.	Open
38.	GAO-19-412R, #19-05	Establish and implement policies or procedures, or both, to provide reasonable assurance that the video surveillance systems at all IRS facilities record activity at the correct time and are properly secured. The policies or procedures should include periodic checks and adjustments, as needed, as part of the annual service and maintenance of security equipment and systems.	Open
39.	GAO-19-412R, #19-06	Update and implement policies or procedures, or both, to clarify (1) who is responsible for conducting the annual review of the visitor access logs, (2) the date by which the review is to be conducted, and (3) how the review should be documented.	Open
40.	GAO-19-412R, #19-07	(1) Identify the reason IRS's policies and procedures related to the transmittal forms were not always followed and (2) design and implement actions to provide reasonable assurance that SB/SE units comply with these policies and procedures.	Open
41.	GAO-20-480R, #20-01	Update and implement policies and procedures for developing a courier contingency plan to prohibit managers responsible for overseeing the preparation of taxpayer receipts for deposits from also transporting them to financial institutions.	Open

Legend:

AEHR: All Events History Report
 AMC: Audit Management Checklist
 CO: certifying officer
 IAT: Integrated Automation Technologies
 ICO: Input Correction Operation
 IDRS: Integrated Data Retrieval System
 IRM: Internal Revenue Manual
 IRS: Internal Revenue Service
 ISRP: Integrated Submission and Remittance Processing
 KISAM: Knowledge Incident/Problem Service Asset Management
 P&E: property and equipment
 PVS: Processing Validation Section
 RSN: refund schedule number
 SB/SE: Small Business/Self-Employed
 SCC: service center campus
 SPS: Secure Payment System
 USR: unit security representative

Source: GAO. | GAO-21-401R

Enclosure III

Enclosure III

Comments from the Internal Revenue Service



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

April 21, 2021

Ms. Cheryl E. Clark
Director, Financial Management and Assurance
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C., 20548

Dear Ms. Clark:

I am writing in response to the Government Accountability Office (GAO) draft, Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls (GAO-21-401R). We are pleased that GAO acknowledged our progress in addressing our financial management challenges and agreed to close forty-eight prior year financial management recommendations. The enclosed response addresses the new recommendation, which we accept.

The IRS continues efforts to improve financial systems internal controls and information technology security by implementing initiatives that address the root causes. We appreciate this acknowledgment in the IRS's FY 2020 and FY 2019 Financial Statements audit opinion (GAO-21-162).

Notably, during FY 2020 we successfully implemented both the Families First Coronavirus Response Act and the CARES Act, and we timely completed the financial statement audit despite the challenges posed by the COVID-19 pandemic.

We are committed to implementing improvements dedicated to promoting the highest standard of financial management, internal controls and information technology security. If you have any questions, please contact me, or your staff can contact Teresa Hunter, Chief Financial Officer, at 202-317-6400.

Sincerely,

Charles P. Rettig
Digitally signed by Charles P. Rettig
Date: 2021.04.21 08:13:38 -04'00'

Charles P. Rettig

Enclosure

Enclosure

**GAO Recommendations and IRS Responses to
GAO FY 2020 Management Report:
Internal Revenue Service Needs to Improve Financial Reporting and Information
System Controls Enclosure I
(GAO-21-401R)**

Recommendation 1, External System Controls and Risk Were Not

Adequately Assessed: The Commissioner of the Internal Revenue Service should reasonably assure that reviews of external third parties' systems reference current documentation that supports IRS assessments of risk.
(IRS reference 21R-01)

Comments: The IRS agrees with this recommendation.

- The Chief Financial Officer will update the external third parties' systems review procedures to reasonably assure that the reviews reference current documentation that supports IRS assessments of risk.

Due Date: August 15, 2021

- The Chief Financial Officer will implement updated procedures to reasonably assure that the external third parties' systems reviews reference current documentation that supports IRS assessments of risk.

Due Date: November 15, 2021

Enclosure III

Text of Comments from the Internal Revenue Service

Page 1

April 21, 2021

Ms. Cheryl E. Clark

Director, Financial Management and Assurance

U.S. Government Accountability Office 441 G Street, NW

Washington, D.C., 20548

Dear Ms. Clark:

I am writing in response to the Government Accountability Office (GAO) draft, Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls (GAO-21-401R). We are pleased that GAO acknowledged our progress in addressing our financial management challenges and agreed to close forty-eight prior year financial management recommendations. The enclosed response addresses the new recommendation, which we accept.

The IRS continues efforts to improve financial systems internal controls and information technology security by implementing initiatives that address the root causes. We appreciate this acknowledgment in the IRS's FY 2020 and FY 2019 Financial Statements audit opinion (GAO-21-162).

Notably, during FY 2020 we successfully implemented both the Families First Coronavirus Response Act and the CARES Act, and we timely completed the financial statement audit despite the challenges posed by the COVID-19 pandemic.

We are committed to implementing improvements dedicated to promoting the highest standard of financial management, internal controls and information technology security. If you have any questions, please contact me, or your staff can contact Teresa Hunter, Chief Financial Officer, at 202-317-6400.

Sincerely,

Charles P. Rettig

Enclosure

Page 2

Enclosure

GAO Recommendations and IRS Responses to GAO FY 2020 Management Report: Internal Revenue Service Needs to Improve Financial Reporting and Information System Controls Enclosure I

(GAO-21-401R)

Enclosure III

Recommendation 1, External System Controls and Risk Were Not Adequately Assessed: The Commissioner of the Internal Revenue Service should reasonably assure that reviews of external third parties' systems reference current documentation that supports IRS assessments of risk.

(IRS reference 21R-01)

Comments: The IRS agrees with this recommendation.

- The Chief Financial Officer will update the external third parties' systems review procedures to reasonably assure that the reviews reference current documentation that supports IRS assessments of risk.

Due Date: August 15, 2021

- The Chief Financial Officer will implement updated procedures to reasonably assure that the external third parties' systems reviews reference current documentation that supports IRS assessments of risk.

Due Date: November 15, 2021

(104634)